Remarks by the Director of National Intelligence Ambassador John D. Negroponte

Overseas Security Advisory Council Department of State – Washington, DC

November 15, 2006

AS PREPARED FOR DELIVERY

Thank you for that very kind introduction, Ambassador Griffin.

Ladies and Gentlemen: It's a pleasure to be here with you this morning.

As you all know, we find ourselves in an extended period of transition and turmoil that commenced with the end of the Cold War and is likely to continue well into the future. These are dangerous times.

We in the Intelligence Community are concerned about terrorism.

We are concerned about the spread of weapons of mass destruction.

We are concerned about conflict and instability in Iraq, the Middle East, and elsewhere.

And we are especially concerned about threats to US citizens pursuing business, humanitarian, cultural, academic and other interests throughout the world.

The Intelligence Reform and Terrorism Protection Act of 2004 therefore gave my office a mandate that I can sum up in a single sentence: Integrate the foreign, military, and domestic dimensions of US intelligence into a unified enterprise that meets the highest standards of objectivity, accuracy, and timeliness.

In other words, the U.S. Intelligence Community is charged with discovering and sharing information that is necessary to defend our nation, our values and our citizens, whether those citizens be troops, diplomats, or private citizens abroad with every expectation that they will receive their government's vigilant support.

In this regard I would highlight information sharing above all other elements of our efforts at intelligence reform. In today's world, nothing can move faster than information and nothing can enlist the constructive efforts of more diverse institutions and individuals than timely, relevant, objective information. We do have to develop new institutions in the War on Terror – the National Security Branch of the FBI and the National Counterterrorism Center, for example – but safety starts with communication.

Indeed, the information sharing challenge extends far beyond the Intelligence Community's sixteen agencies to encompass the Federal government; the state, local, and tribal level; and you in the private sector as well. As a result, our office is pursuing two new organizational features that are helping drive information sharing forward.

The first is the establishment of the Information Sharing Environment Program Manager, a position held by former ambassador Ted McNamara. The PM ISE has been a part of our senior team since June 2, 2005, when the President directed that the Program Manager fall under the "authority, direction, and control" of the DNI. The Intelligence Reform and Terrorism Prevention Act of 2004 created the PM/ISE to "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties...through the use of policy guidelines and technologies."

Faced with a plethora of existing systems, not to mention myriad studies and surveys on the U.S. Government's terrorism information sharing capabilities, the PM ISE dedicated most of its first year to baselining these capabilities to ensure that our analysis was grounded in solid assumptions about the U.S. Government's existing capabilities.

Now Ambassador McNamara has completed an Implementation Plan Report that includes a recommended design for the information-sharing environment. He also has rolled out "blue pages" as part of its electronic directory services that will provide agency contact information for all agencies with counterterrorism responsibilities in the federal government. Yellow and white pages, including more specificity, will follow these blue pages.

The second organizational change in the information area is the establishment of an IC Chief Information Officer as a Senate-confirmed member of the ODNI's senior leadership team. This is a major plus for the Intelligence Community and underpins virtually every aspect of intelligence reform. Our CIO, Major General (ret.) Dale Meyerrose, appointed in December 2005, already has been successful at breaking down barriers to information sharing and implementing information sharing standards. By dismantling prohibitive firewalls, he has expanded access to critically important Sensitive But Unclassified information. And he is our point person in ensuring that the FBI's National Security Branch and the Department of Homeland Security's Office of Intelligence and Analysis are able to interact collaboratively with their IC colleagues anywhere in the world. This means that Regional Security Officers, Legal Attaches, and others are better plugged-in to intelligence products than was the case just a few years ago.

Strengthening American intelligence also means recognizing that we in the government don't have a monopoly on wisdom. Secretary George Shultz acknowledged as much when he established OSAC 21 years ago to foster collaboration between the private sector and the US Government on security threats abroad. In a less formal but no less critical manner, we in the Intelligence Community have begun to engage the private sector to address the challenges of our time. Just last week, my office hosted a daylong, unclassified workshop on energy security with some of the brightest lights from government, industry, and NGOs. The idea is radically simple: get smart people together, put them in a room, have them debate strategic issues that will develop

over the next 15 to 20 years, and see what kind of ideas they come up with. What we get as a result is that most precious of all assets: fresh thinking. Over the next year, we're planning to host several more of these workshops – on emerging technologies, political and economic stability in China, and failed states, among others.

As we pursue these new initiatives, we must not lose sight of the crucial importance of protecting privacy and civil liberties. This is sensitive work in a nation with our distinctive political culture and traditions. We are bringing intelligence to America in a way that has never before been attempted – or been necessary. But it's necessary now. Our Civil Liberties Protection Officer is therefore deeply involved in all of our information-sharing activities, in full coordination with his IC counterparts. Where rules, policies and processes have to be amended or created as a means of protecting civil liberties in this new age of information sharing and access, it falls to him to alert me to the issue.

By the same token, if you see something that you think could be damaging to our national security at home or abroad, please let law enforcement and our embassy Regional Security Officers know your concerns. In fact, even before you spot trouble, I would strongly suggest you establish close communication with our embassies' commercial counselors, our consular officials, and your local American Chamber of Commerce. Don't be shy about getting to know the Chief of Mission, either. Speaking from experience, I know the Chief of Mission will welcome the opportunity to meet you and learn about your activities and projects. Being abroad together brings out the teamwork in Americans, so take advantage of all the well-informed networks and support mechanisms you can. Your active participation in the American community abroad before something untoward happens may help stave off such an event, or at least help you mitigate and manage its effects.

The unitary nature of maintaining security in a globally interdependent system is such that getting together here in Washington is only half the challenge – getting together in the field on a regular basis is the other half.

So keep communicating, keep sharing information, and stay in touch. There's no better way to make sure we all stay safe.

Now I would welcome your comments and questions. Thank you very much.